HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,699	03/04/2002	David F. Bantz	YOR920010530US1	4789

29683 7590 02/21/2006

HARRINGTON & SMITH, LLP
4 RESEARCH DRIVE
SHELTON, CT 06484-6212

EXAMINER	
WILLIAMS, JEFFERY L	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 02/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/090,699	BANTZ ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/25/2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *3/4/02* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 11/25/05.

All objections and rejections not set forth below have been withdrawn.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1 and 25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 1, the term "actual data" is a relative term which renders the claim indefinite. The term "actual data" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. Data, such as would be processed (without understanding) by a computer, is the raw material by which information is derived. The examiner asserts that the implied degree of data, as claimed ("actual data"), is indefinite, as data acts as data depending upon the relative

viewpoint of one who interprets the data. In other words, the information derivative of data is relative in nature, depending upon the context and understanding of a human who interprets the data. See definitions of "data" and "information", Microsoft Computer Dictionary, 3rd ed., 1997. Thus, one of ordinary skill in the art is unable to determine what markings could possibly be displayed that would not, under any circumstances, be material (data) from which some amount or type of information could be derived.

For purposes of examination, the examiner presumes the applicant to refer to "data used to convey information within the encrypted file".

Regarding claim 25, it is found to be indefinite for similar reasons as claim 1. It is unclear how "the information" (the meaning of data) can be displayed to a user as "markings, jumbled text, jumbled numbers, and symbols that does not represent actual data" (lines 8-10). The examiner asserts that if any such markings (jumbled text, jumbled numbers, and symbols) are displayed, then data will have been displayed regardless. Additionally, it is further unclear, as to how a determined meaning of data, "the information" - derived from the encrypted information, can simply be displayed as any arbitrary form of data (markings, jumbled text, jumbled numbers, and symbols), as is implied by the claim language.

For purposes of examination, the examiner presumes the applicant to refer to "if the predetermined decryption key has not been received from the key FOB, displaying data on the display screen as one of the group consisting of markings, jumbled text,

jumbled numbers, and symbols that does not represent data used to convey the information".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 – 4, 6, 9, 10, 13, 15, 17, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nii, "Method for Providing Multimedia Files and Terminal Therefor", U.S. Patent Publication 2002/0076051 A1 in view of Kori et al. (Kori), "Signal Transmission Apparatus and Signal Transmission Method", U.S. Patent Publication 2001/0037307.

Regarding claim 1, Nii discloses:

a display device comprising an electrical display, a file with encrypted information, a system for displaying the encrypted information on the display, and a decryption key receiver; and a key FOB adapted to transmit a decryption key to the decryption key receiver of the display device, wherein the display device is adapted to

display the encrypted information on the display in a decrypted form when the receiver receives the decryption key from the key FOB (Nii, fig. 2, elem. 40; page 3, par. 27; page 5, pars. 62,63). Nii discloses a IC card ("key FOB") that transmits a decryption key to a terminal that displays a decrypted file only after receiving the decryption key from the key FOB.

Nii does not disclose that when a proper decryption key is not received, the system will display markings other than the decrypted data. In other words, Nii does not disclose *and wherein the display device is adapted to display markings other than actual data on the display when the receiver does not receive decryption key from key FOB*. However, it would have been obvious, based upon logical reasoning, to visually display markings such as messages, images, shapes, or types of visual markers that might be interpreted as such that the decryption key for decrypting the data desired by a user has not been provided to the system, or would otherwise be seen in place of desired content. Furthermore, this method was well known in the art of content display systems. For example, the content display system of Kori discloses that a display unit should display markings (scrambled content) other than the decrypted content desired by the user when the system is not provided with the correct decryption key (Kori, par. 30, 40).

It would have been obvious to employ the method, such as taught by Kori, for displaying markings other than desired decrypted data when a proper decryption key has not been received within the system of Nii. This would have been obvious, because one of ordinary skill in the art would have been motivated by logic and well known

practices to securely display content only when a proper decryption key has been received.

Regarding claim 2, Nii discloses:

wherein the display device comprises a computer and the electrical display comprises a computer screen (Nii, fig. 2, elem. 40, 130).

Regarding claims 3 and 4 and 6 Nii discloses:

wherein the key receiver comprises a radio frequency decryption receiver, wherein the decryption key receiver comprises a wireless receiver , and wherein the key FOB comprises a wireless transmitter for transmitting the decryption key to the decryption key receiver (Nii, page 5, par. 62). Nii discloses that the Key FOB and key receiver interface is "contactless", thus a wireless radio interface as evidenced by Dudek et al., U.S. Patent Publication 2003/0018532, page 1, par. 6.

Regarding claim 9, Nii discloses:

wherein the key FOB comprises means for transmitting a plurality of different encryption keys, and means for periodically changing the decryption key transmitted the decryption key receiver (Nii, page 2, par. 19; page 5, par. 67; page 6, par. 7; fig. 7, elem. 64). Nii discloses that a plurality of files ("at least one"), each encrypted with a key, may be accessed by a user with a key FOB. Therefore, the key FOB must possess means for transmitting the corresponding decryption key for the chosen

encrypted file. Thus, Nii discloses transmitting a plurality of different keys as well as periodically changing the decryption key that was transmitted.

Regarding claim 10, Nii discloses:

wherein the display device comprises a memory and a system for temporarily storing the decryption key received by the decryption key receiver in the memory (Nii, page 3, par. 27).

Regarding claim 13, it is rejected, at lest, for the same reasons as claim 1, and furthermore because Nii discloses:

a frame adapted to be placed at a user's head; a display screen attached to the frame and located in front of a user's eye (Nii, fig. 2, elems. 40, 130). Nii discloses a display screen (130) attached to a frame (40). The frame is placed in the proximity of ("at") a user's head, with the screen in front of a user's eye so as to be seen by the user.

wherein non-encrypted information is always displayed (Nii, par. 82, lines 23-30). Nii discloses that decrypted information ("non-encrypted") is displayed to the user.

Regarding claim 15, it is rejected, at least, for the same reason as claim 4.

Regarding claim 17, Nii discloses:

a second receiver connected to the frame for receiving the information contained within *the encrypted signals* (Nii, fig. 2, elem. 133 – elem. 130).

Regarding claim 25, it is the computer readable medium and instructions implemented by the system of claim 1, and is rejected, at least, for the same reasons.

Claims 7 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nii in view of Doyle et al., U.S. Patent Publication 2003/0159044 A1.

Regarding the claims 7 and 8, Nii discloses a system designed to "assure secure delivery and controlled usage of data". The system incorporates an IC card or "Key FOB" for transmitting a decryption key so as to "adequately assure access only by persons authorized for access to selected multimedia content" (Nii, page 2, par. 18). The system of Nii, however, does not ensure that only the authentic owner of the IC card is able to utilize the IC card so as to transmit a decryption key. Thus, the system of Nii, does not disclose the use of biometric data to ensure only the authentic owner of the IC card may utilize the IC card.

Doyle et al. discloses an IC card or "Key FOB" that comprises a biometric sensor for reading fingerprint data of the user of the card. This ensures that only the authentic owner of the card may utilize the card in a system, "improving security" (Doyle et al., page 9, par. 80).

It would have been obvious to one of ordinary skill in the art to have employed the method of Doyle et al. for integrating an authenticating biometric scanner into an IC card within the system of Nii, which utilizes an IC card. This would have been obvious

because one of ordinary skill in the art would have been motivated to improve security of the system by ensuring that only the authentic owner of the IC card ("Key FOB") may utilize the card.

Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nii in view of Klemba et al., (Klemba), "International Cryptography Framework", U.S. Patent 5,835,596.

Regarding claim 26, Nii discloses a IC device for the storage and processing of secret data (Nii, par. 9, 20, 62-65). Nii does not disclose that the circuit within the IC device self-destructs upon attempts to disassemble the device.

Klemba also discloses an IC devices for the storage and processing of secret data. Klemba discloses that the circuit inside the device will self-destruct upon attempts to disassemble the device. This method protects the secret data inside the device (Klemba, col. 3, lines 22-44).

It would have been obvious to one of ordinary skill in the art to employ the tamper-resistance method of Klemba within the IC device of Nii. This would have been obvious, because one of ordinary skill in the art would have been motivated by security concerns to protect secret data.

Claims 21, 22, and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nii in view of Fairman et al. (Fairman), "Data Communications", U.S. Patent 6,996,722.

Regarding claims 21 and 22, they are the method claims implemented by the system claims of 1 and 6, and are rejected, at least, for the same reasons. However, Nii does not disclose the use of a key seed to generate the decryption seeds within the IC device. Rather, Nii discloses that the decryption keys are pre-generated and stored on the IC device (Nii, fig. 5). Thus, Nii does not disclose *sending a new decryption key seed to a user.*

Fairman discloses the method of sending a decryption key seed to a user IC device, so that the IC device may generate the appropriate decryption keys for any amount fresh encrypted data that is received by the user (Fairman, fig. 5).

It would have been obvious to one of ordinary skill in the art to employ the method of Fairman within the system of Nii. This would have been obvious, because one of ordinary skill in the art would have clearly seen the benefits of flexibility and resource savings. The avoidance of a stagnant set of content keys would allow a user to receive fresh and newly created content utilizing his existing IC device. A user would not have wastefully dispose of an IC device and purchase a new IC device, nor would he have to wastefully refresh an IC device via the transmission/reception of a large data set of new encryption keys, as opposed to a small data seed.

The combination of Nii and Fairman, furthermore disclose that key values are predictable, thus an assumption ("determination") of compromised security. Countermeasures, dictate the sending of fresh seed values, as opposed to stale (predictable) values, in response (Fairman, col. 2, lines 53-60; col. 3, lines 30-33; col. 6, line 63 – col. 7, line 9).

Regarding claim 27, the combination of Nii and Fairman disclose: *wherein the new decryption key seed I periodically changed* (Fairman, col. 3, lines 30-33; col. 9, lines 6-13).

Claims 23 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Nii and Fairman in view of Doyle et al., U.S. Patent Publication 2003/0159044 A1.

Regarding claims 23 and 24, the combination of Nii and Fairman discloses a system designed to "assure secure delivery and controlled usage of data". The system incorporates an IC card or "Key FOB" for transmitting a decryption key so as to "adequately assure access only by persons authorized for access to selected multimedia content" (Nii, page 2, par. 18). The system of Nii and Fairman, however, does not ensure that only the authentic owner of the IC card is able to utilize the IC card so as to transmit a decryption key. Thus, the system of Nii and Fairman, does not

disclose the use of biometric data to ensure only the authentic owner of the IC card may utilize the IC card.

Doyle et al. discloses an IC card or "Key FOB" that comprises a biometric sensor for reading fingerprint data of the user of the card. This ensures that only the authentic owner of the card may utilize the card in a system, "improving security" (Doyle et al., page 9, par. 80).

It would have been obvious to one of ordinary skill in the art to have employed the method of Doyle et al. for integrating an authenticating biometric scanner into an IC card within the system of Nii and Fairman, which utilizes an IC card. This would have been obvious because one of ordinary skill in the art would have been motivated to improve security of the system by ensuring that only the authentic owner of the IC card ("Key FOB") may utilize the card. Thus, the combination of Nii, Fairman, and Doyle et al. discloses:

providing the key FOB with a biometric sensor, and wherein the step transmitting the decryption key from the key FOB occurs after the biometric sensor senses a predetermined biometric parameter of the user and *wherein the biometric sensor comprises a fingerprint sensor, and the fingerprint sensor senses a fingerprint of the user* (Nii, page 3, par. 27; Doyle et al., page 9, par. 80). The combination of Nii, Fairman, and Doyle et al. disclose that only after sensing a proper fingerprint scan may the user utilize the card, sending a decryption key.

Claims 11, 12, 16, 19, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nii.

Regarding claims 11 and 12, Nii discloses a system designed to "assure secure delivery and controlled usage of data". The system incorporates an IC card or "Key FOB" for transmitting a decryption key to a user's multimedia terminal so as to "adequately assure access only by persons authorized for access to selected multimedia content" (Nii, page 2, par. 18). A user may access content on his terminal only after supplying a decryption key that is stored the IC card. Thus, Nii discloses that it is undesirable for a user to access content without being in possession of a proper key transmitted from an IC card. Furthermore, Nii discloses that after a predetermined event, such as the activation of an IC card, the decryption key will expire and be unavailable to the user. Thus, the user would be unable to utilize the decryption key on the IC card for accessing encrypted content on his terminal (Nii, page 5, pars. 62, 64). Nii, however, does not disclose that the decryption key transmitted from the IC card to the user's terminal would be deleted after a predetermined period of time.

However, it would have been obvious to one of ordinary skill in the art, based upon logical reasoning, to cause the decryption key stored on the user's terminal to be deleted, similarly becoming unavailable to the user after a predetermined period of time. This would have been obvious because one of ordinary skill in the art could have recognized that the system of Nii required that a decryption key for displaying decrypted content was to become unavailable to the user after a predetermined period of time.

Therefore, it is only logical to conclude that in order to enforce security and the protection of encrypted content through making unavailable an encryption key, the user should not be able to attain availability of the key via access to a stored key by any means. Thus, as the decryption key on the IC card was to expire and prevent access to protected content, likewise, it would have been obvious for the same key on the terminal to expire (be deleted as an equivalent), preventing its use to access protected content.

Regarding claim 16, it would have been obvious to one of ordinary skill in the art for the memory to comprise volatile memory. This would have been obvious, because one of ordinary skill in the art would have been motivated for the purpose of security to prevent a decryption key from being permanently stored within the terminal where it could be used to access protected content without the IC card.

Regarding claims 19 and 20, they are rejected for the same reasons as claims 11 and 12.

Claims 5, 14, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nii as applied to claims 1 – 4, 6, 9, 10, 13, 15, 17, 21, 22, and 25 above, and further in view of Ronzani et al., U.S. Patent Publication 2002/0163486 A1.

Regarding claims 5 and 14, Nii discloses a system designed to "assure secure delivery and controlled usage of data". The system incorporates an IC card or "Key FOB" for transmitting a decryption key so as to "adequately assure access only by persons authorized for access to selected multimedia content" (Nii, page 2, par. 18). The system of Nii comprises a frame comprising a screen for securely displaying data only to authorized users (Nii, fig. 2). Nii, however, does not disclose that the display comprises a frame, such as an eyeglass frame, adapted to be placed on user's head, and wherein the electrical display comprises a screen adapted to be located in front of the user's eye.

Ronzani et al. discloses a display comprises a frame, such as an eyeglass frame, adapted to be placed on user's head, and wherein the electrical display comprises a screen adapted to be located in front of the user's eye. The frame could also comprise earphones to enable a listener to privately hear content (Ronzani et al., fig. 1). Such a display apparatus is useful for "numerous applications including commercial, industrial, and entertainment purposes." It is beneficial to employ in situations where private and detailed viewing of the display is desired (Ronzani et al., page 1, par. 5; page 4; par. 98).

It would have been obvious to one of ordinary skill in the art to employ the head mounted display apparatus of Ronzani et al. in the system of Nii for securely displaying data only to authorized users. This would have been obvious because one of ordinary skill in the art would have been motivated for the purpose of security to enable only an authorized viewer of protected content to privately view the content without the risk of

unauthorized viewers eavesdropping or shoulder-surfing so as to gain access to protected content.

Regarding claim 18, Nii discloses a system designed to "assure secure delivery and controlled usage of data". The system incorporates an IC card or "Key FOB" for transmitting a decryption key so as to "adequately assure access only by persons authorized for access to selected multimedia content" (Nii, page 2, par. 18). The system of Nii comprises a frame comprising a screen for securely displaying data only to authorized users. The display and receiver to the display of Nii is connected by wire to a terminal. (Nii, fig. 2). Nii does not disclose a wireless connection to the display and display receiver.

Ronzani et al. discloses a wireless arrangement for the connection of a display and display receiver (Ronzani et al., page 1, par. 7; page 2, par. 13; page 9, par. 165). This wireless arrangement conveniently allows the display apparatus to be adapted to be placed on user's head, and wherein the electrical display comprises a screen adapted to be located in front of the user's eye. Thus the viewer of the display is enabled to view content from a remote source. This wireless arrangement also allows a listener to privately hear content transmitted from a remote source via earphones (Ronzani et al., fig. 1). Such an arrangement is useful for "numerous applications including commercial, industrial, and entertainment purposes." It is beneficial to employ in situations where private and detailed viewing of the display is desired (Ronzani et al., page 1, par. 5; page 4; par. 98).

It would have been obvious to one of ordinary skill in the art to employ the wireless arrangement for the connection of a display and display receiver of Ronzani et al. in the system of Nii for securely displaying data only to authorized users. This would have been obvious because one of ordinary skill in the art would have been motivated for the purpose of convenience and security to enable only an authorized viewer of protected content to privately view the content from a remote source without the risk of unauthorized viewers eavesdropping or shoulder-surfing so as to gain access to protected content.

Claims 28 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination Nii and Ronzani, and further in view of Fukushima et al. (Fukushima), U.S. Patent 6,123,661.

Regarding claim 28, the combination of Nii and Ronzani discloses a head mounted display, but does not disclose *wherein the frame comprises a sensor for sensing when the frame is removed from a user's head.* Fukushima discloses a head mounted display comprising sensors that would detect when a frame was removed from a users head (Fukushima, col. 1, lines 54-58; col. 8, line 30 – col. 9, line 20). Herein, Fukushima discloses a head mounted display comprising sensors for detecting a user's pulse and visual activity via a sensory connection with the user's head. If the detection of the user's pulse or visual activity falls below a certain threshold, (i.e. such as would happen when the sensory connection with the user's head is broken - frame removed)

then the head mounted display will shut down to conserve power. It would have been obvious to incorporate the sensory features of Fukushima within the system of Nii and Ronzani. This would have been obvious because one of ordinary skill in the art would have been motivated to prevent the waste of system power and prevent the unwanted exposure of sensitive information by deactivating the display device when it is not in use by the system user.

Regarding claim 29, the combination of Nii, Ronzani, and Fukushima discloses the deactivation of the display of decrypted information when the system is not in use by the user (see claim 28). However, the combination does not disclose *wherein the decryption key is deleted upon sensing that the frame has been removed from the user's head.* However, it is reasonable that when the decrypted information is no longer needed, the decryption key is likewise no longer needed. Thus, one could conserve system resources (i.e. storage space) and protect system security (i.e. prevent the likelihood of stolen keys) by removing decryption keys that are no longer in use by the system. It would have been obvious to one of ordinary skill in the art, based upon logical reasoning, to utilize such a method within the combination of Nii, Ronzani, and Fukushima. This would have been obvious because one of ordinary skill in the art would have been motivated by the need to conserve valuable resources (i.e. memory) and prevent unnecessary risks to security (i.e. stolen keys which were no longer in use).

Response to Arguments

Applicant's arguments with respect to claims 1 - 29 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Claims 1 – 29 are pending.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
AU: 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER